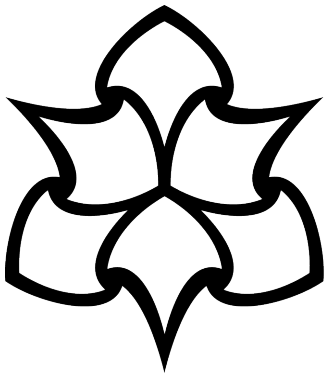


DATA-DRIVEN POLICING: THE HARDWIRING OF DISCRIMINATORY POLICING PRACTICES ACROSS EUROPE

PATRICK WILLIAMS AND ERIC KIND

european network against racism aisbl

Published by the European Network Against Racism (ENAR) in Brussels,
in November 2019, with the support of the Open Society Foundations.

Design and layout: www.emilysadler.com

ENAR - European Network Against Racism aisbl
Tel: +32 2 229 35 70
Email: info@enar-eu.org
www.enar-eu.org

With the support of the Rights, Equality and Citizenship Programme of the European Union, the Joseph Rowntree Charitable Trust and the Sigrid Rausing Trust.

CONTENTS

APPROACH

This report was prepared by Patrick Williams and Eric Kind with the support of the Open Society Foundations. The project was managed by Rebekah Delsol, from the Open Society Justice Initiative, and Becky Hogge, from the Open Society Foundations. The report benefited from the advice and guidance of an advisory panel consisting of:

Rosamunde von Brakel, Vrije Universiteit Brussel

Sarah Chander, European Network Against Racism

Hannah Couchman, Liberty

Lina Dencik, Cardiff University

Claire Fernandez, EDRi

Joshua Franco, Amnesty International UK

Vera Franz, Open Society Foundations

Katrina Ffrench, StopWatch

William Isaac, DeepMind

Fieke Jansen, Cardiff University

Gerbrig Klos, Amnesty International NL

Michael Shiner, London School of Economics

Eric Töpfer, Deutsches Institut für Menschenrechte

A meeting of the advisory board members helped shape the direction of the report, and a convening of anti-racist advocates and campaigners provided feedback to the key messages of the report which were presented by the authors. A number of interviews with advisory board members helped provide key information, particularly about practices in different jurisdictions, which underpinned the research findings of the report.

FOREWORD

We, as activists, as anti-racist organisations, and as racialised communities in Europe, know too well what it means to be over-policed and under-protected. Still, in 2019, we feel the need to evidence racial profiling, to contest narratives placing us as a threat to 'security' and essentially to unsettle presumptions as to our criminality.

We are still mastering the techniques with which we contest over-policing, brutality and racial profiling. We must now contend with another challenge. When law enforcement resorts to new technology to aid their practice, we find ourselves at further risk. Not only must we consider our physical safety in our relations with the authorities, we also need to be informed about the security of our data.

The use of systems to profile, to surveil and to provide a logic to discrimination is not new. What is new is the sense of neutrality afforded to data-driven policing. This report opens a conversation between all those invested in anti-racism, data privacy and non-discrimination in general. It is crucial that we use our collective knowledge to resist.

Karen Taylor, Chair,

European Network Against Racism (ENAR)

INTRODUCTION

Across Europe we are witnessing the increased use of technologies to assist policing and wider law enforcement practices. While some of these technologies are not new, law enforcement's increased resort to data sharing and analytics, and predictive policing tools to direct policing resources has concerning implications for minority ethnic and marginalised communities.

Law enforcement agencies present technology as 'race' neutral, independent of bias, and objective in their endeavour to prevent crime and offending behaviour. Such claims overlook the overwhelming evidence of discriminatory policing against racialised minority and migrant communities across Europe. For people of African, Arab, Asian and Roma descent, alongside religious minority communities, encounters with law enforcement agencies of many European countries are higher than for majority white populations. Whether in interactions with the police or numbers in prisons, European criminal justice systems are policing minority groups according to myths and stereotypes about the level of 'risk' they pose, rather than their behaviour.

This report explains the potential effects of the increased use of data-driven technologies for minority groups and communities. It combines our collective understanding of criminological processes of criminalisation with information about the incursion of new technologies into contemporary policing. There is an urgency to consider the potential (mis)uses of data-driven police technologies for racialised minority groups. At present, we face (public and private) organisational silences that conceal technology from public scrutiny and accountability. This is further complicated through ongoing debates concerning the reliability, validity and/or ethics of data use upon which much of these new tools are based.

Within this report, 'hardwiring' refers to the process of incorporating historical and prospective police and law enforcement data into technology to support the policing function. We argue in this report that the introduction of new technology is negatively impacting ethnic minority communities in three ways:

1

The impact of new technologies to identify, surveil and analyse will be **disproportionately felt by minority ethnic communities**, as they are already over-policed. This includes crime-analytics as well as the use of mobile fingerprinting scanners, social media monitoring and mobile phone extraction among others.

2

Many algorithmically driven **identification technologies disproportionately mis-identify people from black and other minority ethnic groups**. For communities that are already over-policed, such technological limitations, found for example in facial recognition, will increase further the likelihood of discriminatory stop and search, due to technological misidentification(s).

3

Finally, predictive policing systems are likely to **present geographic areas and communities with a high proportion of minority ethnic people as 'risky'** and subsequently, foci for police attention. Predictive policing systems, responding to calls for improvements in crime detection, have been developed based upon data that reflects ethnic profiling and racist policing. This will result advertently in the 'hardwiring' of historical racist policing into present day police and law enforcement practice.

The presence of new technologies both assists and drives over-policing by providing law enforcement agencies with risk-making capabilities, alongside developing databases which contain racialised stereotypical assumptions of minority communities.[1]

The report has three main sections. Firstly, we set out disparities in policing based on ethnic, nationality and religious categories across Europe. We take as our starting point ethnic profiling as intrinsic to European law enforcement practices and in so doing utilise key concepts such as suspicion, risk and 'risk-making', and the racialised tendencies of criminalisation.

The second section gives a high level overview of the 'surveillance industry' responsible for developing policing technologies, with a discussion of its role in the policing eco-system, and their claims of scientific objectivity and technological ('race' and ethnic) neutrality. We introduce a broad spectrum of policing technologies, conceptually grouped as identification technologies; data harvesting and network mapping technologies; database fusion, enrichment and analysis tools; and then predictive policing tools. We include discussion of facial recognition, automatic number plate recognition, voice print identification, finger-print identification, social media monitoring, the use of telephone call detail records, mobile phone extraction, IMSI catchers, body worn cameras, data sharing and the creation of new databases, and both person based and place based predictive policing tools.

We feature case studies throughout to emphasise particular practice by a police force in a certain country serving to highlight the implications of data-driven technologies for maintaining racial profiling and discriminatory policing practices. In noting the cumulative and racialising risk-making effects of data-driven technology, we focus attention on technologies that drive the 'criminalising communities' and 'crime anticipation systems'.

We envisage that this report will help set out the basic information about the harms of racialised police practices and the potentially harmful effects that data-driven technologies present. The report concludes by identifying some future challenges and opportunities for activism, areas that need further research, and recommendations for action as initial steps in building resistance against the hardwiring of discriminatory policing practices across Europe.

RACIAL DISPARITY IN POLICING

Ethnic, nationality and religious disparity across Europe

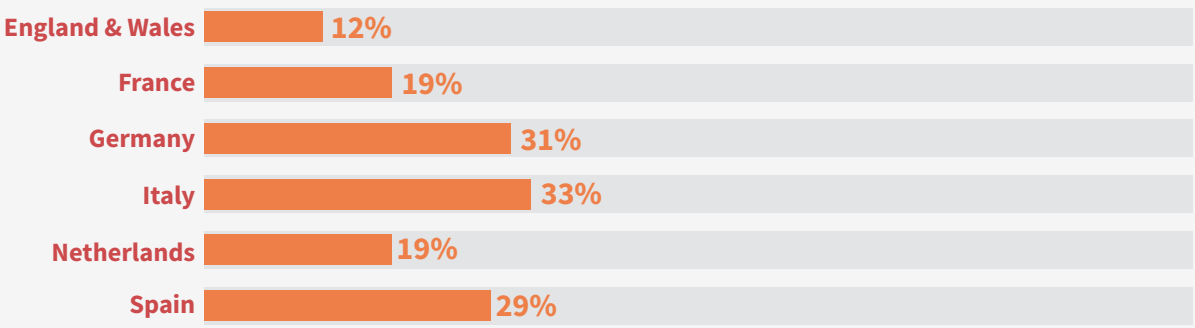
Across Europe, minority ethnic groups and communities consistently report experiences of over-policing by police and law enforcement agencies. Most recently, the UK government commissioned Lammy Review confirmed the existence of a 'racial disparity' characterised by increased rates of stop and search, prosecution, punishment and imprisonment for minority groups and communities when compared to the 'majority' population.[2] Such findings are clearly replicated across Europe where 'foreign nationals' are over-represented in prisons (see chart below).

Added to this, evidence from the EU Fundamental Rights Agency shows that 14% of respondents to the survey were stopped within the preceding 12 months, with 40% indicating this was due to their 'immigrant or ethnic minority background'.[3] In England and Wales, black people are more than nine times more likely to be stopped and searched by the police, a figure that increases to over twenty times in particular areas in England and Wales.[4] Collectively, the 'black'[5] group were at greatest risk of being stopped and searched by the police - where in Austria, a majority (66%) of Sub-Saharan African respondents were stopped by the police within the preceding five year period. The same applies to 38% of black people in Finland and 30% in Lithuania. People of North African background were subject to significant levels of police stops in France (31%), Italy (32%), Netherlands (33%). For those of South Asian background in Greece, the figures are 59%, in Cyprus 43% and 22% in Italy. Just under half of Roma people in Greece (47%) were stopped, with 46% of respondents in Spain, and 45% in Hungary.[6]

Beyond the personal and emotional effects of over-policing (to be discussed below), it is important to recognise the criminalising effects of targeted profiling. In particular, these practices afford the police and law enforcement agents with opportunities to gather information about certain communities based on the assumption that they present a heightened risk of criminal activity. By 2005, the UK government had established what was regarded as the largest DNA database in the world upon which the details of 135,000 black males aged between 15 and 34 years of age were held, representing three-quarters (77%) of the overall database.[7] On the one hand, this serves to illustrate the high levels of stop and search and the gathering of DNA information and further demonstrates the reality of ethnic profiling as an intrinsic feature of policing.

To be stopped and searched and/or subject to over-policing is not a measure of criminality or the propensity to crime, but rather, the state's formal response to (ethnic, religious and nationality) groups who are presented as 'outsiders' and as not belonging to the country within which they reside. Therefore, it is necessary to consider the conceptual ideas that drive the over-policing of minority groups.

Proportion (%) of 'foreign nationals' in prisons

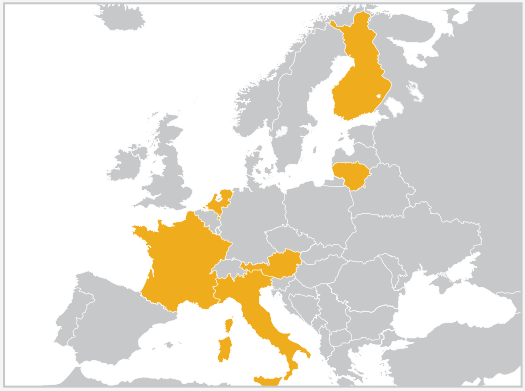


Source: Aebi, M.F. et al (2018) 'Foreign offenders in prison and probation in Europe: Trends from 2005 to 2015 (inmates) and situation in 2015 (inmates and probationers)'. University of Lausanne: Council of Europe.

In **England** and **Wales**, figures indicate that **black people** are more than nine times more likely to be stopped and searched by the police, a figure that increases to more than twenty times in particular areas in England and Wales.

% of respondents that were stopped by the police within the preceding five year period:

Sub-Saharan African



Austria 66%
Finland 38%
Netherlands 33%
Italy 32%
France 31%
Lithuania 30%

South Asian

Greece 59%
Cyprus 43%
Italy 22%

Roma

Greece 47%
Spain 46%
Hungary 45%

Ethnic profiling drives the over-policing of minority groups and communities

Dominant discourses on ethnic profiling often focus on (a) the inadequacy of monitoring and data collection practices by European law enforcement agencies and (b) the heterogeneity of racialised groups across Europe, which restricts the ability to develop and apply general explanations for stop and search practices across different European countries.

While we accept the basis of such arguments, the everyday reality alongside the personal and emotional harms of intrusive policing practices have wider repercussions for minority groups and communities. There has long existed political anxieties that minority communities are responsible for driving up social problems, including crime and offending behaviour within European countries, with specific racial, ethnic and/or religious groups being pathologised as possessing and posing 'risks' of criminal activity due to either socio-economic status, cultural or religious differences and/or affiliations. However, evidence clearly shows that minority populations commit criminal offences at a similar, and more often than not, at a lower rate than the majority population.[8] Despite this, that particular groups are more likely to be stopped by police is better understood as a politically-sanctioned policed response to groups who law enforcement officers 'suspect' as being involved in criminal activity.

To be stopped and searched then is not a random event, but a state driven daily occurrence for minority people across Europe. Of more concern, explanations of police racism and discriminatory law enforcement practices are increasingly concealed behind political claims of immigration control, the 'cultural incompatibility' of minorities in Europe and broader crime control (including serious violence, extremism, illegal immigration).

Before moving on to discuss the surveillance industry the following will highlight the critical ideas which drive ethnic profiling and over-policing across Europe.

FROM SUSPICION TO RISK

"I remember a time, I think it [was] Year 9 or Year 10… I was getting stopped every week. Without a doubt, I'd get stopped all the time. At that time, I didn't really chill in my area…[I]t was weird man. Starting to get stopped and searched all the time to the point where it became a joke. It was just a normal thing like putting on your clothes.[9]

In assessing how law enforcement are using new technology to further embed racialised stereotypes and assumptions into policing practices, it is important to de-construct how data is used to construct ideas of 'suspicion' and 'risk' for racialised communities.

"When you're stopped when you're not doing anything suspicious, and you're stopped without the reason even being explained, that creates a really bad feeling. And you feel a lot of fear inside. You ask yourself, 'Is there something wrong? Has someone said something about me? What is happening, exactly?' A few hours afterwards, you're still thinking about it, especially if they ask you for your name. You think, 'Well, what are they doing with my name? They think I did something? Why did they ask for my name, specifically? Am I going to be stopped somewhere else after that?[10]

Suspicion as a driver of police stop and search practice is well documented.[13] Media representations and commentaries of 'crime' serve to amplify and communicate racist stereotypes which evoke and heighten the majority groups' suspicion of racialised minority groups.

"There was a moment in which it didn't affect me because it was so normalized, I saw it through this prism. 'Well it's normal, I am Gitano and that's why they stop me.' There is no documentation that can show that they stopped you for a racial profile if they say it's routine, security, suspicion.[11]

Crime prevention and criminal law enforcement is increasingly discussed in terms of risk-management, characterised as the development of technology solutions alongside the introduction of actuarial forms of risk assessment to control specific groups of 'risky' people and to manage a plethora of risks assumed to be faced by the populations of advanced societies.[14] It is important to recognise that cultural depictions of crime and risk influence the reality of law enforcement and the construction and operation of risk categories.

Of additional concern, algorithmic risk predictor tools are increasingly used to target groups and individuals who are calculated as posing a high level of risk who in turn are increasingly more likely to populate 'suspect lists' and to determine the level of punishment they will receive.

"During the checks, what do I think about? As it is, when this happens, there are always people walking around. People start staring at you. 'What is Adil doing with the police?', 'What are those guys doing with the police?' or 'What do the police want with them?', 'What have they done this time?' How do the police see me? They just see me as a Moroccan, like all the other Moroccans, and that just makes you feel really bad. It's like you have to scream for your rights even though they are doing you wrong. That feeling is really frustrating. It destroys something inside of you. I don't feel protected by the police. It's more like I feel I have to protect myself from them in some situations. They don't listen to you as a citizen in those situations. It's because people, the police, paint that picture again: 'Yes, it's a Moroccan.'[12]

"Stop and search - Zekarias" by EYE DJ is licensed under CC BY-NC-ND 2.0

RACIALISED CRIMINALISATION

Criminalisation refers to a process where law enforcement agencies infer criminality on the behaviours, traits or characteristics of a group, behaviours that in isolation are non-criminal. Processes of criminalisation enable policy makers and law enforcement agencies to define what behaviours are criminal and should be policed. However, rather than focusing upon what governments may decide are problematic behaviours, campaigners should be alert to and where necessary, challenge the definitions of crime being handed down by the state. Our question should be, 'what factors (political, economic, law enforcement policy, etc.) result in defining specific behaviours as criminal?' In asking such questions, we can reveal the particular groups being targeted by contemporary law enforcement policies and practices.

Recently, policing has drawn attention to specific youth behaviours as problematic. For example, while it is not a criminal offence to be in a 'gang', to appear in a Rap, Grime or Drill music video, or to perform in a music video, such behaviours are increasingly being viewed with *suspicion of criminality*. Criminologically, such behaviours have been understood as expressions of youth culture, youth political engagement and young people's group-identity. However, today such behaviours have been constructed as legitimate targets for policing and law enforcement surveillance. Law enforcement increasingly resort to social media to gather information about these behaviours. It was recently reported that the police are able to trawl social media for images and content, with such 'fishing' activities generating vast data. In 2018, the London Metropolitan Police was reported as having a database of 1400 videos[15] with Amnesty International suggesting that the content of this database is not always gathered using appropriate legal protections for human rights.

Racialisation refers to the process of attributing negative characteristics to groups based upon their belonging to a specific ethnic group. Racialisation recognises power relations as a historical socio-political feature of any given society and therefore helps us to understand why different groups at different times are portrayed as problematic in different European countries.

As part of racialised criminalisation, technology is being used by law enforcement agencies to support and justify the collection of 'non-criminal' information about individuals and their associations (friends, family members, romance links, etc.) who may engage in such behaviours. In turn, this data becomes central to profiling and intelligence building practices through the development of priority or suspect lists that include the identification and surveillance of racialised non-criminal individuals. The contentious practice of social media monitoring, facial recognition technology online and/or in public spaces, data capture through police body worn cameras, all contribute data to the development of such lists.

The racialisation of specific crime-types and forms of offending behaviour are portrayed as specific to particular minority ethnic groups. Offence types such as drug dealing, theft, street robbery, religious extremism, radicalisation, street gangs, serious violent crime (knife crime) are (wrongly) communicated as particular to minority ethnic groups and communities. Within a number of European jurisdictions, young black and brown people are increasingly being targeted and registered onto police gang databases as 'suspects' or gang nominals which advertently marks them out for police attention and increased police encounters.[16] Academics have long argued that the racialisation of gangs creates 'useful enemies' who have become 'a lightning rod for broader social anxieties during moments of [national] uncertainty, resulting in intensive securitisation and efforts at moral regulation'.[17] Similarly, the particular law enforcement attention upon Muslim communities across Europe as posing a 'risk' of extremism and radicalisation again serves to illustrate how racialised criminalisation has facilitated the introduction of technologically driven policing, which disproportionality impacts religious minority people and communities.

CASE STUDY 1: GANGS AS STRATEGIC SUBJECTS

Despite the absence of a clear European wide definition, social researchers have noted the emergence of government policy in response to collectives of mainly young people in specific countries. In the Netherlands it is estimated that there are 1,154 gangs members while in Spain, there are reportedly three types of gangs, namely the 'extreme right', 'extreme left' and 'Latin bands'. In France, there were reportedly 222 gangs in 2009, comprised of some 2,500 individuals which had increased to 313 gangs by 2011. Within England and Wales, there are upwards of 3,800 gang nominals whose details are recorded on a bespoke gangs database which is managed by the London Metropolitan Police.

RESPONSES TO THE 'GANG'?[18]

» In Spain, the government established the police coordination and intervention plan against 'organised violent juvenile groups' which included 'increasing intelligence on gangs through mapping and monitoring; cross-agency training on gang issues; increasing contact with teachers, parents and young people; setting up of government advisory groups and improving collaboration within criminal justice settings including prisons'.[19]

» In France, a 'gang shut down strategy' to be driven by amongst other approaches, called for 'increasing the intelligence within areas exposed to the [gang] problems by making use of real time intervention'.

» In Portugal, law enforcement professionals reported a significant issue with juvenile gangs. Positive approaches to the 'problem' were reported as 'working with youngsters and their families in the community, for example in socially deprived areas where youngsters are at higher risk of becoming involved in violent offending and participating in gangs'. Here, intervention programmes were concentrated (again) in 'at risk' communities.

» Denmark and Sweden have dedicated multi-agency 'gang' management units which have been significant in driving up the numbers of minority groups who are made subject to gang interventions.

Whilst the above does not infer the minority status of those who are deemed to be involved with gangs, research highlights the racialising tendencies in the European attention to the phenomenon of gangs.[20] What emerges is a reluctance across European jurisdictions to discuss the ethnicity of 'gang' members or those who were thought to perpetrate youth violence. Despite this, the study found that young people from immigrant backgrounds were significantly over-represented in the youth justice system of France, the Netherlands and Sweden. In Sweden, practitioners were more inclined to discuss the growing inequality between rich and poor and the similarly growing (economic) inequalities between young people of Swedish and non-Swedish background. In the Netherlands, gang suppression strategies have focused attention upon Moroccan descent communities, with some acknowledgement of how strategies need to be 'culturally-sensitive' for racialised minority and religious groups in gang figures. In London, approximately 78% of those recorded to the police gang database are from a black minority ethnic background.

Despite some ambiguity in acknowledging the racialisation of police-defined gangs across Europe, a study undertaken in 2006 indicated the following:

'Students of American gangs are used to hearing of Hispanic and black gangs, while less commonly of Asian or white. In Europe, the street gangs are also primarily composed of ethnic or national minorities, reflecting the immigration and refugee patterns of those countries. Indigenous street gangs are reported in Holland, Norway, Denmark, Germany, Russia and Italy, but the more common gangs are composed of Algerians, Moroccans, Turks, Indians, Pakistanis, Jamaicans, Chinese and Albanians, among others.'[21]

CASE STUDY 2: CRIMINALISING COMMUNITIES

The hardwiring of racialised criminalisation has resulted in members of ethnic, national or religious minority groups all being viewed and surveyed with a presumption of criminality. As such, individuals who are members of such communities, irrespective of whether they are engaged in criminal behaviour or not, can be made subject to police and law enforcement attention simply due to their membership of the suspect community.

Alarmingly, in Denmark, the emergence of the highly contentious practice of criminalising communities can be found in the establishment of 'ghetto lists', ghetto zones or 'harsh penalty zones' in 2018 wherein individuals who are found guilty of an offence will be subjected to 'double punishment' compared to individuals who do not live within geographically defined ghetto zones. By way of clarity, an area is ascribed harsh penalty zone status where it matches at least three out of five of the following 'social criteria':

» The population is more than **50% non-Western immigrant**.

» More than 2.7 % of inhabitants have **criminal convictions**.

» **Unemployment** is above 40%.

» More than 50% have only a **basic education**.

» Inhabitants' **average gross income** is less than 55% of the average of the region.[22,23,24]

Of significance here, the dominant criteria for inclusion within a 'zone' is not related to the rates of crime within the geographical area, but appear driven by a political reaction to the concentration of 'non-Western immigrants'. The move towards criminalising communities marks the deliberate effort to regulate the estimated 28,000 immigrants who are thought to be concentrated in 'ghettos' who are constructed as resistance to integration to Danish society's norms and values. The specific groups for attention are noted as those of predominantly 'Somali or Lebanese background'. As part of the implementation phase, the policy makes direct reference to the introduction of 'monitoring and surveillance' within ghetto zones, seemingly to facilitate the speedy prosecution and conviction of 'offenders'.

'The effect of these [harsh penalty zone] laws will be clearly racist, and discriminatory on grounds of religion. It is one thing to promise increased policing of high-crime areas. But to make such crimes as vandalism, burglary, threatening behaviour, arson and offences against the drug laws punishable by twice the sentences when committed within the designated ghettos is just grotesque.' [25]

Central here is a presumption of criminality and the attribution of stigma to communities racially defined as 'ghettos' and through which negatively racialised groups reside. Of further concern is the isolation of the variable and particularly the '50% non-western immigrant' measure which once calculated will 'hardwire' discrimination and ethnic profiling into policing practice and drive the police to police minority communities differently. The consequence of this is that, where law enforcement investigations are enacted, then the technology serves to assist risk-making and will support the speedy prosecution and conviction of minority immigrant individuals within such communities. The technological drivers for policing in this regard are numerous but explicitly serve to drive the policing or minority groups and to increase the notoriously low conviction rates that exist across European countries.

POLICING TECHNOLOGIES

The use of technology to support and advance policing is not new. Whether the technology is employed to assist law enforcement agencies with managing the information they already hold, or to collect new information, as the pace of technological development has increased so has police appetite to make use of technology. As a result, there is a wide spectrum of ways in which law enforcement agencies use technology. Within the following, we summarise technology that, despite potential racialising effects, is acknowledged as assisting the policing function. Obvious tensions in the development of assistive technologies will become apparent; law enforcement increasingly use them against or in communities presumed to be 'criminal', but also, as we will develop later, they serve law enforcement agencies in the exploitation of data gathering mechanisms to enhance pre-existing data sources.

The surveillance industry

The companies building surveillance tools for law enforcement arguably have more in common with defence contractors than the technology sector. A report by NGO Privacy International[26] shows the global surveillance industry is overwhelmingly based in economically advanced, large arms exporting states, with the US, UK, France, Germany and Israel comprising the top five countries in which the companies are headquartered. A number of companies were founded by former intelligence or law enforcement agents and many employ high numbers of former government personnel.[27]

Due to the specialised nature of the tools they develop and sell, the majority of companies providing technologies to law enforcement will not be household names.[28] There are some exceptions to this, such as where companies are developing multi-purpose technologies that could be deployed in a number of different sectors. One example is NEC whose facial recognition technology[29] is used commercially as well as by the public safety sector, or the provision of cloud services such as Amazon Web Services which are used widely by companies, but is also the platform of choice for the deployment of the UK's new nationwide police intelligence database.[30] Some companies, such as Axon, have made decisions not to sell face-matching products as part of their body-worn cameras[31] due to ethical concerns, while others like data analytics company Palantir have refused to cancel lucrative contracts with U.S. Customs and Immigration Enforcement despite the ramping up of punitive immigration policies.[32]

Technology is not neutral?

It is often argued - including by technology developers themselves - that technology is neutral or amoral. However, this proposition ignores the intentions of those who design and produce technology. Technology does not simply come into existence, immaculately conceived and purposeless. Instead it is a product of its time, with all the political and social influences this brings. Often companies design technology with specific purposes in mind, such as solving a specific 'crime' challenge, possibly for a police client, and inevitably incorporating many of the client's ideas and assumptions. Rather than seeing technology as neutral or amoral, it is more accurate to see it in its wider context: that its development was likely by a company, possibly founded by a former intelligence or law enforcement professional, to sell to other intelligence law enforcement bodies, primarily to make a profit. With that in mind, rather than seeing the creation and adoption of a new kind of technology in the area of policing as neutral act, we should view it in the same way as any other new policy or development in policing.

Due to the high level of involvement of former law enforcement professionals in designing technology for law enforcement, it is probable that assumptions of suspicion, risk and (racialised) criminalisation influence the design and the broader organisational understandings of crime. To illustrate, drawing upon a noteworthy study,[33] law enforcement perceptions of criminality, including what geographical areas were perceived as criminal was informed by a 'corporate memory' which is culturally specific to the local law enforcement agency. The corporate memory means that, rather than being objective or neutral, policing practice is organisationally informed by past experiences and attitudes as well as what is or is not remembered. The same study found that police officers believed that

'high intensity' areas for serious violence were those that were characterised by high ethnic heterogeneity. This view persisted even in light of contradictory evidence presented to the police based on police recorded crime. In other words, the police officers' perception of 'unsafe areas' was premised upon the 'concentration of minority ethnic people', suggesting that the presumption of criminality is driven more by 'what is remembered' and concealed within the corporate memory of the police and law enforcement agents.

The development of technological fixes to 'crime problems', particularly when the technology is premised upon racialised police assumptions, may simply perpetuate pre-existing human biases and social inequalities. The belief in the independence and objectivity of data-driven policing solutions and in particular, predictive policing programmes will send law enforcement officers to monitor and detect crimes in the same already over-policed communities.[34]

Source: West Yorkshire Police, available at: https://www.westyorkshire-pcc.gov.uk/media/137136/img_28121.jpg

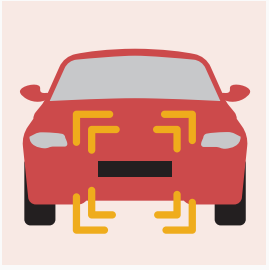
Who is this? Identification technologies

Identifying individuals has always been a key part of police work. Modern police services now have a number of different tools and technologies at their disposal to answer the question 'who is this person?' This includes facial recognition, automatic number plate recognition, voice print identification and the increasing use of mobile finger-print identification. This section will briefly introduce some of the key technologies deployed by law enforcement against ethnic minority communities.

FACIAL RECOGNITION

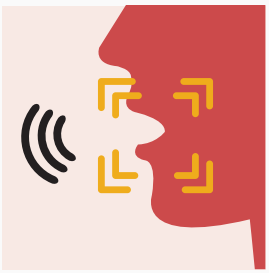
The public and private sector continue to use video surveillance systems (or CCTV) to monitor spaces. These systems are fundamentally the same as they were when they were introduced.[35] What has changed is the advent of new analytic capabilities, seeking to make use of the captured video imagery. The ability to do this, affordably and at scale, fundamentally increases the intrusiveness of these tools. Video analytics can automate the identification of people in day-to-day life. Capabilities to identify people by their 'gait' (how they walk and move), are being referenced in governmental strategy documents[36] but the most publicised of recent new capabilities is the increased use of automated facial recognition technology.

Automated facial recognition technology can detect faces in an image or video and compare it to other databases to attempt to identify individuals. Police who are deploying high-resolution cameras in public spaces use it to identify individuals on a watch list or suspect list in real time. Studies show that automated facial recognition technology disproportionality misidentifies women and people from black and minority ethnic groups.[37] This means that police are more likely to wrongfully stop, question and possibly arrest them. There have been trials of the use of automated facial recognition technology in public spaces in the UK where individuals who tried to hide their faces from the camera were stopped for 'suspicious behaviour'[38] and issued with a public order fine. Early deployments of facial recognition in the UK include events that serve minority ethnic communities and most notably the Notting Hill carnival for the identification of 'persons of interest'. In Germany, police have retrospectively searched video footage from the G20 summit protests[39] to try to identify protesters before the State Data Protection Commissioner of Hamburg stopped the practice.[40] There have been some evaluations of automated facial recognition tools by police[41,42] and the practice is currently subject to legal challenge in the UK.[43] Public authorities in San Francisco, the City of Oakland, and Somerville, Massachusetts have all voted to ban the use of facial recognition technology by city agencies including police departments.[44]



AUTOMATIC NUMBER PLATE RECOGNITION

Police are also increasingly using automatic number plate recognition (ANPR). ANPR cameras are physically installed to record passing cars, and use optical character recognition to convert number plates to digital text, which can then be cross-checked against national police and driver databases. While these technologies have not changed much since they were introduced more than fifteen years ago[45] there are new proposals to link these systems with other existing video surveillance systems, and join together the analytic capabilities, including those from automated facial recognition systems.[46] ANPR cameras record cars passing through a checkpoint, or if enough ANPR cameras are deployed, act as a real-time record of cars moving through the road network and their location. While ANPR cameras are in common use across Western Europe,[47] there has been limited discussion about the potentially discriminatory ways these cameras can be used. There are concerns that cars can be 'marked', leading to increased stop and search, made possible due to ANPR-triggered traffic stops.[48] The Brandenburg police used the example of looking for "motorhomes or caravans with Polish license plates" in a recent leaked internal evaluation of the system.[49] The ability to search for license plates of a particular nationality, and indeed looking for 'motorhomes or caravans' is highly suggestive of a potentially discriminatory focus on Travellers or Roma.[50,51]



SPEAKER IDENTIFICATION

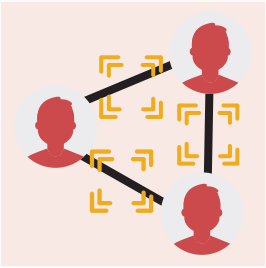
Police are also increasingly exploring using other forms of biometrics such as speaker identification. It should be noted the difference between speaker identification which identifies who is speaking, and speech identification which identifies what is being said. Speaker identification works by taking samples of a known voice, and then converting key features of the voice into an algorithmic template known as a voice print or voice model. There is little knowledge about individual police services' practices with speaker identification at the national level, however police forces in the UK, Portugal and Italy have been involved in pilots.[52] Intelligence agencies have used voice biometrics for at least a decade at significant scale,[53] and at the international policing level there are some high profile efforts such as Interpol's recently completed Speaker Identification Integrated Project.[54] The Interpol project will provide a shared voice biometric database for 192 police forces. The tool goes beyond identifying a speaker; it filters voice samples by gender, age, language, and accent. Police forces using the technology can upload intercepted phone calls, recorded audio, or search against voices on social media. Such biometrics can be captured in a number of ways, including for example via YouTube. This makes them much easier to acquire than other forms of biometrics, such as DNA for example. For individuals sharing videos of themselves, most would not realise that their voices (and potentially faces) are being turned into biometric prints that might later be used by police to identify them. Studies looking at speech recognition tools found significant gender and racial biases.[55,56]

MOBILE FINGERPRINT TECHNOLOGY

Finally, mobile fingerprint technology are transforming another long used police capability; to identify individuals using fingerprints. With an app on a law enforcement agent's phone and a handheld scanner, police are able to check fingerprints against existing police and government databases (including immigration records) in real time. In Germany the technology has been in use for over a decade,[57] and in the United Kingdom trials are taking place in London[58] and Yorkshire.[59] Agencies do not provide figures of the ethnic breakdown of those whose fingerprint is being checked or taken using these systems, but given the racial disparity of those stopped and searched, and the disparity of previous biometric databases like DNA databases,[60] it is likely that the use of this tool will disproportionately affect minority ethnic communities.

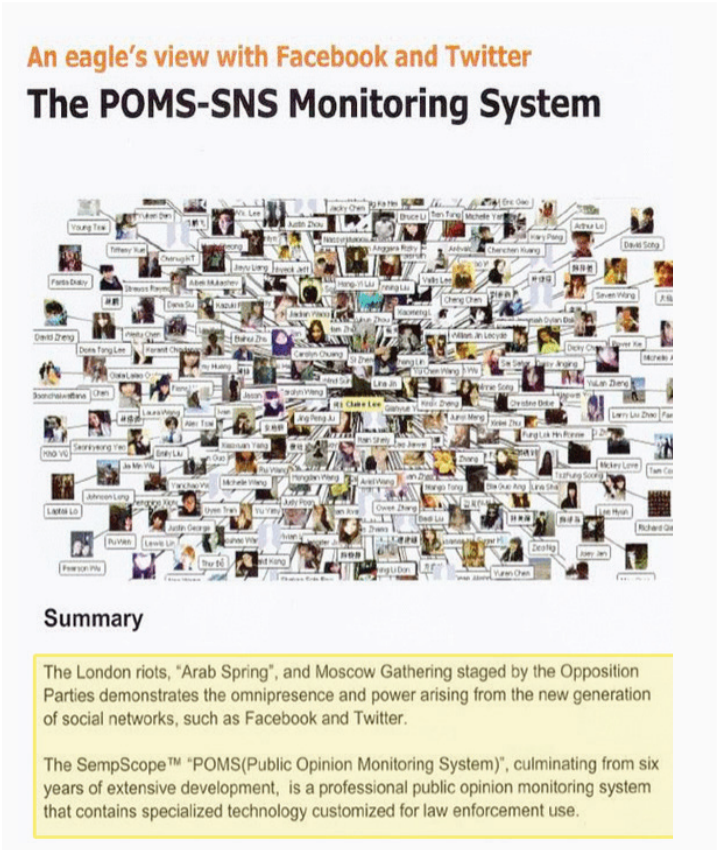
Who knows who? Data harvesting and network mapping

Police are using a range of technologies to try to build a picture of social interactions and relationships. These are all designed to build intelligence and to help answer the question 'who knows who?' In pursuing suspects or individuals who the police and law enforcement officials may think of as suspicious, such technologies can be used to try to tie groups of individuals to each other. In the context of collective forms of punishment, the use of these techniques to build or confirm associations between individuals and groups is an attempt to demonstrate criminal networks and relationships for the purpose of prosecution. There are a number of tools police may use to do this, including social media monitoring, the use of call detail records, mobile phone extraction, IMSI catchers and body worn cameras.



SOCIAL MEDIA MONITORING

Police forces are increasingly conducting social media monitoring to gather information about what is happening on social networking platforms like Facebook or Twitter. It includes online public interactions, but also those happening in private groups. This can be as simple as a police officer browsing the 'public facing' parts of social media websites, to creating a fake persona to infiltrate private groups, to scraping or acquiring social media information in bulk to try to mine the data for connections.[61] In the UK, social media is used to keep track of 'gang associated individuals', and if a person shares content on social media that refers to a gang name, or to certain colours, flags or attire linked to a gang, they may be added to a gang database according to research by Amnesty International.[62] Similarly, police regularly monitor videos on social media to identify links and associations between different individuals. Given the racialisation of gangs, discussed above, it is likely that such technology will be deployed against minority ethnic people and groups.


An eagle's view with Facebook and Twitter

The POMS-SNS Monitoring System

Summary

The London riots, "Arab Spring", and Moscow Gathering staged by the Opposition Parties demonstrates the omnipresence and power arising from the new generation of social networks, such as Facebook and Twitter.

The SempScope™ "POMS(Public Opinion Monitoring System)", culminating from six years of extensive development, is a professional public opinion monitoring system that contains specialized technology customized for law enforcement use.

Sales brochure for social media monitoring tools. Available at: https://sii.transparencytoolkit.org/docs/Semptian-Technologies_POMS_Brochure_1sii_documents.

CALL DETAIL RECORDS

Police can also use 'call detail records' (CDRs) of mobile phones to build a picture of who knows who. These records originated as billing records generated by mobile phone providers when service was provided on a per minute or per text basis, and now are required to be retained throughout Europe under data retention laws. They record the 'to, from, where and when'.[63] These CDRs are held by mobile phone companies and can be requested by police services, usually only after independent authorisation. Requesting the call detail history of an individual immediately provides the police with an extensive view of someone's network or social graph by analysing call, text, and location history.

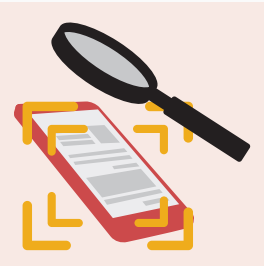
IMSI CATCHERS

Other tools, like IMSI catchers, can also be used to identify everyone who attended a particular place at a particular time. An IMSI catcher[64] is a surveillance tool that works by pretending to be a legitimate mobile phone tower, which can then be used by police forces to achieve a number of different goals. IMSI catchers work in different ways, which means that there is a variation in how different police services use them, however, there are a number of common features including identification, interception,[65] blocking[66] and locating.[67]

An IMSI catcher can force your mobile phone to relay an IMSI number, which is unique and tied to your sim card, and its IMEI number,[68] which is tied to a physical handset or mobile device. Once acquired, police services can link this to your identity by either contacting your mobile phone provider or comparing it against other databases already acquired. This is further assisted if the country has SIM card registration requirements in place, as many countries across Europe do.[69]

IMSI catchers are mostly used as tactical tools, having to be physically on site, and have a limited range. Historically they have been very bulky and were often deployed in vans, but modern IMSI catchers can be no larger than the size of a small backpack, and body-worn versions that are worn under clothing also exist.[70]

Other tools can be used in the place of IMSI catchers if the goal is simply to block calls such as mobile phone jammers,[71] or the police could require the telephone company to shut down the network in a particular geography.[72] Different police forces have different policies in relation to the secrecy of IMSI catchers. In the United Kingdom, police still neither confirm nor deny their use, whereas in Germany, the technology is avowed and deployments are reported annually to the Bundestag.[73] Because of their secrecy, there are no independent studies of how police are using IMSI catchers.



MOBILE PHONE EXTRACTION

With physical access to your mobile phone, police are able to extract all the information held on the device, including deleted data, data stored in the cloud, and data you didn't realise was being collected by your phone. There are a number of ways that law enforcement tools seek to achieve this. If the phone is unlocked, they are able to extract the information directly. If the phone is locked, with strong device encryption, then there are tools that allow the police to hack your phone to gain access to the internal data. There are concerns about the police seizing mobile phones in the context of a stop and search and the legality of extracting data mobile phones.[74]

Depending on the brand and model of the seized phone, how recently the phones' software was updated, and which extraction tool the police are using, the police will gain access with varying success. The information that can be extracted from a mobile phone[75] includes all phone contacts, messages, photos, web browsing history, location history, as well as potentially data used in apps and services such as Facebook, WhatsApp, Twitter and others. Whilst there are no independent studies on the use of these tools, there have been reports by civil society organisations like Privacy International into their use by police.[76]

One area for further consideration is that protections for individuals are often weakest at the border, where police have more lenient search powers and are increasingly using mobile phone extraction technologies as part of their work policing borders. Even if, once searched, nothing is found, the data can be held, and it can be bulk uploaded into a central database to be accessed in the future. In the United Kingdom, the intelligence agencies received a copy of every phone downloaded at the border over the previous month.[77] Given the racial disparity (discussed earlier) in who is stopped at the border it is of particular significance. There are no statistics in the UK for how many times police undertake data extraction, nor is there oversight of racial disparity in their use.

The use of mobile phone extraction is a formidable threat to privacy, and indeed is the single easiest way for police to gather huge quantities of information about an individual's private life, who they know, where they have been, and indeed, potentially where they will be in future.[78]

BODY WORN CAMERAS

Body worn cameras are wearable video cameras, usually visible and mounted on the chest or the shoulder of a police officer. Different cameras have different feature sets with some models recording audio and others only capturing images over a time-lapse period. Many are fitted with pre-record functionality so there is a continuous buffer of the last few minutes of video being recorded which can be stored if the officer presses a button after the event. Others start recording automatically after certain triggers. Police forces across Europe have carried out trials for over a decade now with goals of improving the quality of evidence around incidents, as well as deterring crime. Meta studies suggest that the use of body worn cameras has little impact on officer behaviour as originally expected.[79] Body worn cameras are in use in the UK[80] and the Netherlands,[81] among other European countries. Due to their overt nature, and lack of sensitivity surrounding the technology, there have been a number of studies on the impact and effect body-worn cameras have on both police and citizen behaviour.[82,83,84] The adoption of the tool has split civil liberties organisations, with the American Civil Liberties Union (ACLU) in the United States advocating for use of the tools with accompanying privacy safeguards, and the parallel organisation in the United Kingdom, Liberty, raising concerns about the deployment of the technology, withholding support on the basis of the available evidence.

Concerns have also been raised as to the point at which recordings are initiated by the police. The central focus of police worn cameras as an assistive tool means that the focus of attention is subjectively driven by law enforcement officers rather than an evidential base for ensuring fair and accountable policing. More controversially, the numerous accounts of police brutality captured (or not) on body worn cameras have not facilitated the pursuit of justice. At the time of writing, the inquest into the killing of Rashan Charles by the police during arrest, heard evidence that the police officer did not turn on his body worn camera, which is the procedure in his pursuit of a suspect.[85]

As an image and audio capture platform, police can use these tools to review footage, better identify individuals and build out networks between them and others in frame. The ability for police to run identification and network analytics in addition, including facial and voice recognition, is the inevitable next step for police using this tool.

"Surveillance" by Volker Kannacher is licensed under CC BY-ND 2.0

JERMAINE LEWIS AND THE ENGLISH RIOTS

Jermaine Lewis was one of a group of young black men convicted of riot, possession of a firearm with intent to endanger life, and arson being reckless as to whether life was endangered, for an incident in Birmingham which occurred during the August 2011 disturbances in cities across the UK.

A group of 42 mostly black men congregated outside The Barton Arms pub in the Aston area of Birmingham. Some of the men began throwing furniture from the pub into the road and set the ground floor alight with petrol bombs. Four different firearms discharged at least 12 rounds in the direction of police arriving at the scene and at the police helicopter capturing events on CCTV from above.

Lewis could not be identified on any of the CCTV footage as being at the scene. One of his co-defendants, whom he had met on holiday and who had travelled up to Birmingham, could be identified, but was not seen to engage in any acts of violence. Lewis maintains that he drove his friend and his cousin to the scene and then drove off. The prosecution used cell-site evidence to allege that phones linked to Lewis, his friend and his cousin were in the same general area at around the same times that evening. They then inferred that a break in regular telephone contact between the three phones during this period meant the men were together throughout the evening.

The prosecution brought the defendants' previous convictions and various media reports supposedly demonstrating gang affiliation to the trial. This so-called 'bad character evidence' was intended to show that the defendants had a propensity toward violence involving guns, knew guns were being carried by some members of the group and would be used with intent to kill if necessary, and had negative attitudes towards the police. This enabled members of the group who did not commit acts of violence to be convicted of the offences.

Evidence of gang affiliation mainly revolved around rap videos posted online and pictures downloaded to the defendants' phones, which were interpreted by expert witnesses who were in fact police officers. It was not alleged that any of the defendants were actually gang members. One of the defendants appeared in rap videos associated to a police-defined gang made up of mainly Asian young men and which had not been identified as being a group involved in any specific law-breaking.

Evidence was adduced linking some of the defendants with a gang named the 'Raiders'. A music video featuring alleged members of the Raiders appearing alongside alleged members of the 'Johnson Crew' was presented as evidence of an association between the two gangs.

Members of these affiliated groups were said by the police officers to have a hallmark hand gesture known as 'throwing the sixes'. This hand signal is given in some of the rap videos by some of the defendants. Lyrics referencing 'gang behaviour' were cited by the prosecution. Tattoos with the initials of some of the gang names were used as evidence against some of the defendants.

Lewis appeared in a video called 'Gangbusters R Us' together with his cousin who police identified as one of the gunmen in the trial. The judgement from Lewis' failed appeal states, 'although his role was less prominent, Lewis did spend much of the video in close proximity to [his cousin]'. One lyric refers to a '0.44' and 'Phantom' (Lewis' nickname, or as the prosecution referred to it, his 'street-name'). When this lyric comes up in the video, Lewis mimics a shooting action. On Lewis' phone, a downloaded picture of the emblem of the 'Raiders' along with the word 'menace' was found. Downloaded pictures of guns were also on his phone, as well as one of a hooded man pointing a handgun.

In Lewis' appeal it states, '[he] had no significant criminal history but…he was an active member of the 'Raiders' gang which had used firearms in the past. The video material and that from his phone demonstrated his attitudes to guns and the police. It was pointed out, on his behalf, that he did not have any gun or use any gun.'

Lewis received a sentence of 23 years in prison.

Source: Centre for Crime and Justice Studies (2016)

What do we know? Database fusion, enrichment and analysis

Police forces hold large quantities of information, but are rarely in a position to fully exploit the data they hold. Instead, police data is often managed across multiple separate systems that are not mutually compatible. A recent report by UK think tank RUSI highlights that in the UK "the analysis of digital data is almost entirely manual, despite software being available to automate much of this process".[86] There are few police forces in the UK with tools to analyse unstructured data such as images and video, and consequently there are fundamental limitations as to how the police can use data.

With that said, efforts to remedy these issues are increasing, with only institutional inertia and lack of funding delaying the adoption of new tools. In preparation, more and more police forces are seeking to reorganise their IT architecture to better exploit the information they hold.

In Germany, a project entitled Police 2020 aims to overhaul existing infrastructure and merge all the major databases of federal and state police forces into a single warehouse. Currently led by the state of Hesse, a pilot project provides access to multiple databases via a single search interface.[87]

In the United Kingdom, the National Law Enforcement Data programme is seeking to merge two of the largest databases, the Police National Computer (PNC) and Police National Database (PND). This will include 55.4 million driver records, 54.8 million vehicle records, intelligence files, 12 million images, as well as approximately 10.7 million criminal records.[88]

Other systems in other countries are also increasingly being merged or reconfigured, to provide better access to intelligence that police already hold, but also in preparation for more complex data analysis to be run across the joined databases, or indeed lay the groundwork for future predictive policing systems.[89]

Europe-wide databases are slowly growing in scope such as SIS, the EU's border information management system which includes information on criminal activity, immigration violations and missing persons. New datasets are being integrated, as well as new search functionalities, such as the inclusion of the European wide Automated Fingerprint Identification System (AFIS) and the upgrade to allow searches via fingerprints.[90]

The issues raised by the ability to search for complex information, that might permit analysis against protected characteristics like ethnic profiling, or indirectly via characteristics used as a proxy for ethnicity is poorly studied and there is little to no guidance currently in use by police forces. In 2006, the Constitutional Court of Germany considered the lawfulness of data-mining techniques to try to identify 'sleeper' cells post 9/11 which included discriminating based on protected characteristics. In that case, the court found the practice illegal, but only in the absence of a "concrete danger" to security or lives.[91]

It is likely that further research, legal analysis and guidance is necessary to ensure that police forces are not using ethnic profiling in the course of their increasing data fusion, enrichment and analysis practices.

What will happen? Predictive policing tools

Police use predictive policing programmes to understand and estimate where and when future crimes are likely to be committed - or who is likely to commit them. These are commonly referred to as place-based or person-based prediction tools.

The majority of tools under the banner of predictive policing make general, rather than specific forecasts, and as such may be more usefully labelled as 'forecasting' tools. This is true even of systems with purported capacity to make predictions of crime within the timeframe of a single day.[92]

Looking for trends in crime data has always been part of police work. For some tools, this is merely the continuation of that practice, whilst others go further and attempt to make decisions about what the crime data means, and then forecast where and when crime might happen or who might commit them.

Predictive policing systems necessarily rely heavily on historical data held by police, which can contain biases. 'Biased data' does not mean data that was gathered with bad intentions, or data that will be unfair if used in a certain way. When a system is trained on data that contains bias, any subsequent police method or strategy based upon such data are inclined to reproduce those biases in its results. For example, historical data held by police about crimes is not a record of the levels of crime within any given geographical space, but instead is a record of the crimes that are reported to the police or perhaps a record of events when law enforcement officers have responded to situations in a community. Further, biases can have a 'ratchet effect' meaning that the distortion will get incrementally worse each year if police services rely on the evidence of last year's data in order to set next year's targets.

This has a number of knock-on effects, but an important consequence can be that the police place an over reliance on 'answers' provided by that technology, decreasing the weight of independent scrutiny as a challenge to the technology. Indeed, senior police officers have highlighted that police officers "may lack the confidence and knowledge to question or override an algorithmic recommendation". [93]

There is no central record on the number of police forces using predictive policing tools in any country in Europe, and consequently there is little available information about the types of crimes these tools are being applied to, the companies behind the tools, or continuous assessment of whether they are effective.

Police data works to legitimise the datasets and the police practices that produced them, rendering them seemingly infallible.[94] This is because predictive policing 'rearticulates' police data as 'scientifically valid' and provides law enforcement officials with a 'new vocabulary' to explain the over-policing and the concomitant harms of racialised policing. Whilst for many, police data is assumed neutral, it is evident that the 'entire computational structure' is based upon subjective biases of law enforcement officers. Research studies show that data-driven technologies that inform predictive policing resulted in an increase in levels of arrest for racialised communities by 30%.[95] Predictive technological capabilities also supply law enforcement agencies with a rationale for expanding policing which exacerbates racialised policing.

PERSON-BASED PREDICTIVE TOOLS

Across Europe, media and institutions have consistently constructed the 'gang' as a notion based on the racialised criminalisation of minority groups and communities. The gang has been used as a 'useful suspect' to rationalise the development of data-driven technologies in order to respond to the threat of 'gangs', organised crime groups or youth groups depending upon the jurisdiction.

Arguably, whilst responses to the 'gang' in Europe infer the need for technology either through the monitoring and/or surveillance of 'at risk' communities, it is the racialised dimensions of gang constructions and in turn disparities in the policing of gangs and minority communities that raise particular concern.

Some predictive policing tools use complex machine learning,[96] which makes it difficult to understand the process or model that produced the result, but others use simple algorithms, which can be understood without needing a background in computer science.

For example, the Offender Group Reconviction Score (OGRS) is a predictor of re-offending based on static risk such as age, gender and criminal history to calculate individual predictions. The tool is employed by probation and prison services across Europe and is built upon an algorithm to calculate the likelihood of reoffending (which is expressed as a percentage score). There are key variables that feed directly into the calculation of OGRS, which have the potential to have a discriminatory effect on minority ethnic groups namely, age at first sanction (including warnings, (never) cautions, etc) and age at first conviction. Given the effects of suspicion which result in increased levels of police stops, it is logical that the calculation of their risk of reconviction will be higher, not as a consequence of criminal activity, but as a consequence of the increased likelihood of being stopped by the police and law enforcement agencies.

Consequently, measures of risk within justice contexts are used to determine the level of punishment and intervention dosage that a convicted individual should receive. Typically, the greater the risk (of harm or reoffending) posed, the more intensive and punitive the punishment given. Evidently, higher levels of risk and in turn punishments are more probable for individuals who reside within over-policed communities and consequently, this will disproportionately affect racialised minority communities.

CASE STUDY 3: GANGS MATRIX

The Gangs Matrix is a risk-management tool focused on preventing serious violence run by the Metropolitan Police. It is a database of suspected gang members in London that began as a response to the London riots in 2011 and by 2017 over 3,806 people had been included within the Matrix. There are a number of problems with the system:

» A disproportionate number of individuals on the Matrix are black, indeed, 78% of those on the Gangs Matrix are black, compared to only 27% of those responsible for serious youth violence are black.

» There is no clear guidance or criteria for including individuals onto the Matrix, and researchers at Amnesty documented inconsistent approaches being used by different bodies, with varying threshold levels.

» 40% of people listed on the matrix have no record of involvement in any violent offence in the past two years and 35% have never committed any 'serious offence' despite it being a risk management tool focused on preventing serious violence.

The Matrix isn't an exclusively police tool; 'partner agencies' include housing associations, job centres and borough youth services but there are no legal safeguards around the sharing of data.[97] Individuals are given an automated green, amber, or red violence ranking, and because of the data-sharing this stigmatising 'red flag' can follow people in their interaction with other government agencies causing further problems.

PLACE-BASED PREDICTIVE TOOLS

Place-based predictive systems are designed to assist police in determining the timing and location of police interventions. The United Kingdom has been experimenting with using 'hotspot analysis' called ProMap since 2004[98] and in the Netherlands, a place based predictive tool called the Crime Anticipation System has been used in Amsterdam since 2014.

Usually, place-based predictive tools use historical data held by police departments as the starting point, but some supplement with other data depending on the focus of the system. Programmes have sought to include the weather, socio-economic data of the geographic area, and even the location of off-licences[99] in their calculations. Some systems are acquiring information from data brokers, such as from Experian who have one billion people and businesses in their dataset,[100] and who have been accused of acting illegally in amassing these datasets.[101]

A significant concern for ethnic minority communities is that place-based predictive tools will take data from police records already based on practices of over-policing certain communities, and forecast that based on the higher rates of police intervention in those areas, police should prioritise policing those areas further.

CASE STUDY 4: CRIME ANTICIPATION SYSTEM

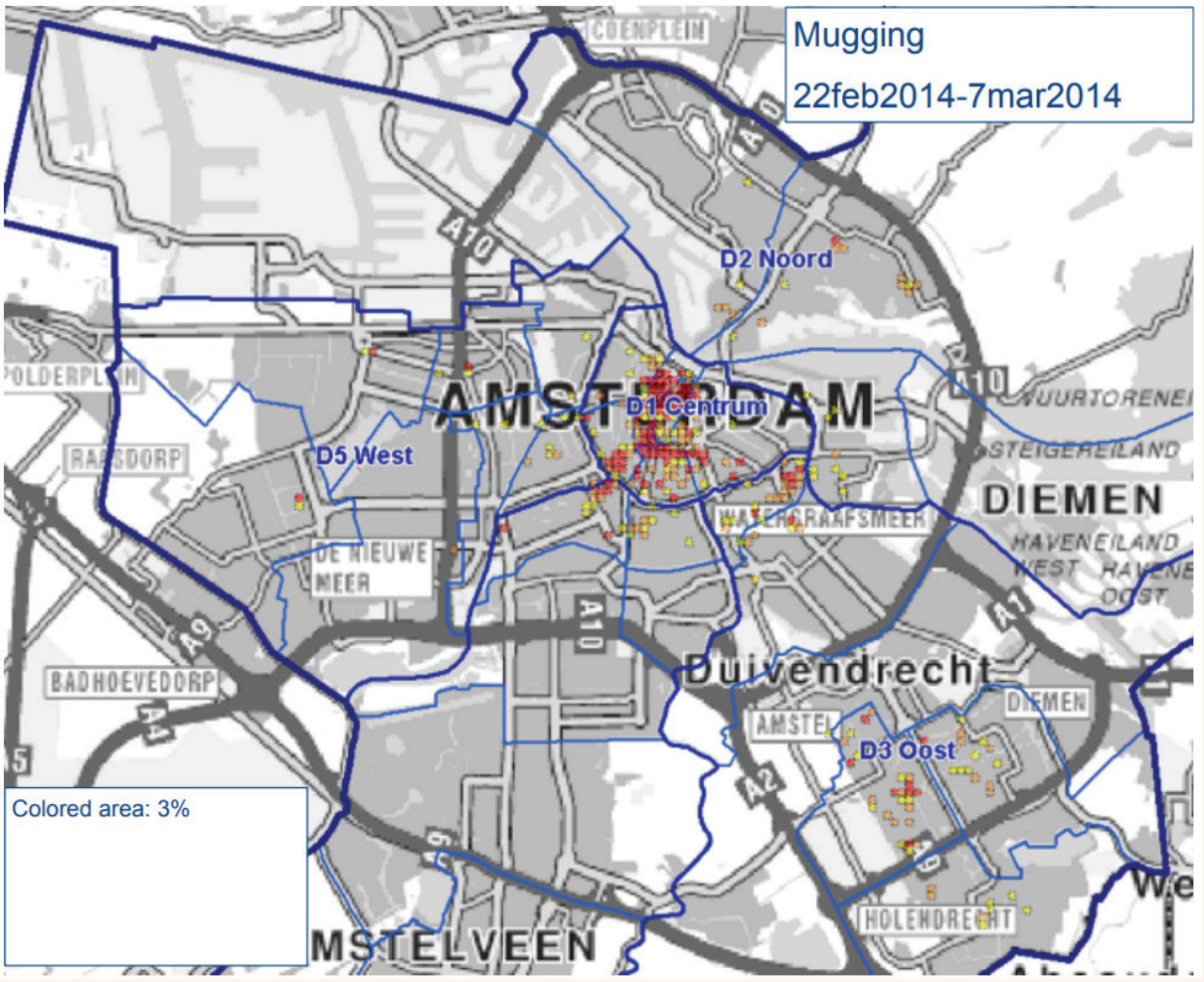
In Amsterdam, the Crime Anticipation System is a place-based predictive policing tool which attempts to predict where specific crimes, such as burglary, muggings and assaults will take place within a two-week period. Amsterdam Police developed the system to predict more at-risk areas in a city, and improve efficient distribution of their workforce. The system uses machine learning to analyse three sources of data:

» socio-economic data from the Central Bureau of Statistics which includes people's age, incomes and the amount of social benefits in an area

» historical crime data, originally gathered by the police, focusing on previous crimes, locations and known criminals

» Geo-data from the Municipal Administration which consists of streets and addresses. This is not used in the model to predict, but rather provides the basis of the map on top of which the predictions sit.

The aim of the analysis is to grade different areas of Amsterdam into red, orange and yellow. Areas that are graded red are considered high-risk and have increased police surveillance deployed to prevent predicted crimes from occurring.[102,103]



An image from the Crime Anticipation System. Source: Willems, D (2014) Presentation: 'CAS: Crime Anticipation System'. Available at: https://event.cwi.nl/mtw2014/media/files/Willems,%20Dick%20-%20CAS%20Crime%20anticipation%20system%20_%20predicting%20policing%20in%20Amsterdam.pdf.

CHALLENGES AND OPPORTUNITIES

Due to excessive secrecy surrounding what the police regard as sensitive capabilities, it can be very difficult to understand the specifics of how many of the tools listed above work or how they are used day-to-day. While there is public information about all the tools mentioned in this report, different police forces do not officially confirm the use of some of them. This can make conversations about the legal basis of usage far more complex than it should be. While there are still many police services who think secrecy is necessary to ensure they can do their work, there are also many who work on the assumption that they have to keep such information confidential, without continually assessing whether that is strictly necessary. Sometimes, the reason for the secrecy stems not from the police, but because the vendors of the tools claim that the algorithms or technology powering the tools is proprietary. This has shielded the tools from scrutiny from the public, the courts, but also in some circumstances the police bodies purchasing the tools.[104] The appropriate response is to seek to force transparency by filing Freedom of Information requests, requiring police services to reconsider their position, release the information or document their position of secrecy.

Alongside Freedom of Information requests, there have been recent efforts by individuals to use data-rights to find out what information police are holding about them and compel the police to delete this information.[105] The claimant in Catt v UK used a 'subject access request' to discover that the police placed him on an 'Extremism Database', and then successfully argued the police should delete this data.

While some of the technology discussed in this report may seem complex, the police are not a technical body (outside of specialist technical teams), and the majority of officers working with the technology will not be technically sophisticated. In part, this is due to the fact that "[t]echnological training is virtually non-existent for police officers" according to the Royal United Services Institute[106] and echoed in Police Federation reports.[107]

Therefore, while police secrecy causes an information asymmetry it does not mean that the police are more technically capable than anti-discrimination activists might be.

It should also not be assumed that all police officers welcome the deployment of these tools. Indeed, some police officers see the introduction of new technology as 'gimmicks'[108] or more profoundly, they recognise that some of these tools will have the potential to fundamentally alter the policing role and how policing operates, and with it, the relationship between police and the communities they serve. With that, there are opportunities for anti-racism campaigners and advocates to work with others who have expertise in technology to identify problems and have equality of arms when discussing them with the police. There might also be opportunities to work with police bodies who recognise that these technologies are no longer top-secret, and that they do not have the moral leadership nor technological expertise to devise by themselves the rules governing how and when new technology should be deployed.

Due to the lack of engagement, transparency and shared language to discuss these tools, there is little scope to discuss them across civil society, policing and academia, or even within the police themselves. Potentially, a consequence of this is the concealment of a reality that technological capabilities that drive policing practice may exacerbate racial disparities in the policing of racialised groups and communities across Europe. Further, there is also a very real concern that the use of technology in policing may make racialised criminalisation more difficult for anti-racist activists and campaigners to (quantitatively) evidence. In the absence of evaluation data or pilot results information to attest to the effectiveness of technology enabled policing, we must consider the future implications that data driven technologies in policing may pose for minority groups and communities.

Finally, whilst technology may be used by police to gather information on citizens, it may also be leveraged by oversight bodies to ensure compliance with the law and anti-discrimination values. It should be possible for databases to be audited by oversight bodies to determine the profile of those whose information the police hold (ethnic breakdown, nationality, geographical location, etc.), and to consider whether there is any racial, ethnic or religious disparity. Audits could go further than just analysing the data holdings, by assessing how the police use the data, including assessing the breakdown of records that police search for, and whether there is the potential for racial disparity at the investigative stage, and at similar steps through the investigation process. Such analyses depend, however, on the availability of data disaggregated by race which differs according to approaches to racial and ethnic data collection across Europe.

CONCLUSION

Racialised policing and ethnic profiling is an everyday experience for minority ethnic people, groups and communities across Europe. The emotional impact is painful, driving mistrust of the police and wider law enforcement agencies and disrupts notions of belonging and citizenship. The introduction of new technologies by police forces in recent years has raised significant questions around the extent to which these tools are further entrenching racial discrimination and criminal injustice. As we have considered throughout, technology is not neutral or necessarily scientifically objective and therefore, unless guarded against, it will exacerbate racial, ethnic and religious disparities in European justice systems.

Whilst we welcome emerging (academic and political) debate and reflection on the accountability and ethics of technology advancement in public life, such debates must take into consideration the realities of racialised discriminatory policing practices, driven by stereotypical assumptions of minority ethnic people.

This report resituates the use of police technology within the context of racial disparity and examines the implications of technological tools when used by police forces where institutional corporate memory drives the over-policing of racialised minority groups. There are today dubious policing practices across Europe as seen in the Netherlands, Belgium and the United Kingdom documented above, driven by the availability and misuse of technology - under the political guise of crime reduction, risk-identification and risk-management. Despite such pretentions, what is self-evident is that the potential for racialised policing to become hardwired, codified and concealed within police and law enforcement technology tools is alarmingly high, increasing further the reality of racialised criminalisation and the potential for wrongful convictions driving up the disproportionate numbers of minority groups in prisons.

The lessons of history show that new technologies will continue to be attractive to police, and as data becomes easier to collect, and as the barriers to adoption fall, the use of such surveillance technology will become widespread. Further research, collaboration, and analysis is desperately needed to respond to these trends, to ensure that such practices are robustly challenged and mitigated against. There is evidently a need to develop rigorous monitoring processes to build European wide understandings of the utility and impact of police technology on minority groups and communities and to hold law enforcement agencies and technology companies to account for the consequences and effects of technology-driven policing. Further, it is hoped that such approaches serve to raise awareness for members of minority groups and communities of the often concealed policing strategies and technologies which continue to drive the over-policing of 'suspicious' communities.

RECOMMENDATIONS FOR ACTION

1. Challenging racialised criminalisation

Challenge and resist the use of stereotypical crime-types and tropes used against negatively racialised communities. The encroachment of police technology is often presented and justified as a need to respond to the threat of 'new' forms of crime and criminal activity. By building collaborations of anti-racist campaigners and critical academics/researchers we can question the evidence base that informs such policing initiatives.

2. Seek guidance to protect yourself

If you believe you are at risk or are being targeted by the police using some of the technologies listed above, consider seeking guidance, legal or otherwise, to help understand and assess what steps could be taken to improve your security. Guidance is available from a number of civil society organisations. This includes guides from the EFF https://ssd.eff.org/; Citizen Lab https://securityplanner.org/#/; and Access Now https://www.accessnow.org/help/.

3. Map what technologies are being deployed by police and law enforcement agencies

While many technologies being deployed by police will be secret (e.g. IMSI catchers), others will be publicly announced (e.g. mobile phone fingerprint scanners). Reports by oversight bodies, academics or think tanks can also provide rich information about what is being used. Mapping the technologies being deployed will allow individuals and communities to be better informed about how they are policed, and help build a Europe wide picture.

4. Identify groups with technology expertise and build networks

Expertise on technology can help fill in gaps in official police explanations, and helps demystify how certain types of technologies are used. There are great European wide networks of digital rights groups,[109] as well as academics[110] working on these issues to build networks with, share information and experiences, and importantly to build resistance to and challenge racist policing.

5. Use freedom of information laws or subject access requests

Through freedom of information laws it is possible to gather information on certain databases or types of technology that police are using. While there are robust exceptions to prevent police disclosing information, if you have questions you want answered, make inquiries as it is always worth trying. Likewise, if you think your information has been captured, and you're on a police database, consider using subject access requests to find out what is held.

6. Organise

When police deploy new surveillance technology or build new databases, consider seeking representation on behalf of your community and ensure your voice is heard. Explore opportunities to make your case to technology companies who are building and deploying these tools as well.

ENDNOTES

1. Williams, P. and Clarke, B. (2018) 'The Black Criminal Other as an Object of Social Control'. Social Sciences, 7: 234.
2. Lammy, D. (2017) 'The Lammy Review: An independent review into the treatment of, and outcomes for, Black, Asian and Minority Ethnic individuals in the Criminal Justice System'. London: HMSO.
3. EU-MIDIS II (2018) 'Being Black in the EU/Second European Union Minorities and Discrimination Survey'. Vienna: EU Fundamental Rights Agency.
4. Home Office (2018) 'Police powers and procedures, England and Wales, year ending 31 March 2018'. London: Home Office.
5. Those of black British, black African and black Caribbean background.
6. EU-MIDIS II (2017) 'Being Black in the EU/Second European Union Minorities and Discrimination Survey'. Vienna: EU Fundamental Rights Agency.
7. Kapoor, N. (2018) 'Deport, Deprive, Extradite'. London: Verso.
8. Bell, B. et al. (2010) 'Crime and Immigration: evidence from large immigration waves'. Centre for Economic Performance, discussion paper, No. 984.
9. Williams, P. (2018) 'Being Matrixed: The over-policing of gang suspects in London'. London: StopWatch.
10. Open Society Foundation and StopWatch 'Viewed with suspicion: The human cost of stop and search in England and Wales'. London: OSF.
11. Neild, R. (2019) 'Under Suspicion: The impact of Discriminatory Policing in Spain'. Open Society Foundation.
12. Open Society Justice Initiative and Amnesty International NL (2013) 'Equality Under Pressure: The Impact of Ethnic Profiling'. New York: OSF.
13. Open Society Foundation and StopWatch 'Viewed with suspicion: The human cost of stop and search in England and Wales'. London: OSF.
14. Feeley, M. and Simon, J. (1992) 'The New Penology: Notes on the emerging strategy of corrections and its implications'. Berkeley Law Scholarship Repository.
15. Waterson, J. (2018) 'YouTube deletes 30 music videos after Met link with gang violence'. The Guardian [ONLINE]. Available at: https://www.theguardian.com/uk-news/2018/may/29/youtube-deletes-30-music-videos-after-met-link-with-gang-violence.
16. Amnesty International (2018) 'Trapped in the Matrix: Secrecy, stigma, and bias in the Met's Gangs Database'. London: Amnesty International UK; Williams, P. (2018) 'Being Matrixed: The over-policing of gang suspects in London'. London: StopWatch.
17. Fraser, A. et al. (2018) 'European Youth Gang Policy in Comparative Context'. Children and Society, 32: 156-165.
18. Fraser, A., Ralphs, R. and Smithson, H. (2018) 'European youth gang policy in comparative context'. Children and Society, 32(2): 156-165.
19. Fraser, A., Ralphs, R. and Smithson, H. (2018) 'European youth gang policy in comparative context'. Children and Society, 32(2): 156-165.
20. Waddell, S. (2013) 'Preventing youth violence: Lessons from three European countries'. London: Winston Churchill Foundation.
21. Klein, M., Weerman, F. and Thornberry, T. (2006) 'Street Gang Violence in Europe'. European Journal of Criminology, 3 (4): 413–437.
22. Fekete, L. (2018) 'Anti-muslim discrimination is now central to Danish immigration and integration policy'. Institute for Race Relations. Available at: http://www.irr.org.uk/news/islamophobia-in-denmark-from-parallel-societies-to-the-ghetto-list/.
23. Ministry of Transport, Building and Housing (2017) 'Ghetto List 2017: Two new areas added, five removed'. [Danish] Government.
24. BBC (2018) 'Denmark plans double punishment for ghetto crime'. Available at: https://www.bbc.co.uk/news/world-europe-43214596.
25. The Guardian (2018) 'The Guardian view on forcible integration in Europe: this cannot end well'. Available at: https://www.theguardian.com/commentisfree/2018/jul/08/the-guardian-view-on-forcible-integration-in-denmark-this-cannot-end-well.
26. Privacy International (2016) 'The Global Surveillance Industry'. Available at: https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

27. This is apparent on the face of the profiles of many company founders, but a detailed sectoral analysis has not taken place.
28. E.g. Palantir, ETI, Elaman, Cobham, Cellxion, Smith Myers, etc.
29. See: https://www.nec.com/en/global/solutions/safety/face_recognition/NeoFaceWatch.html.
30. See the description of the new system in the relevant Home Office procurement document: https://www.digitalmarketplace.service.gov.uk/digital-outcomes-and-specialists/opportunities/7556.
31. Axon (2019) 'The Future of Face Matching at Axon and AI Ethics Board Report'. Available at: https://www.axon.com/company/news/ai-ethics-board-report.
32. Birnbaum, E. (2019) 'ICE renews contract with Palantir', The Hill. Available at: https://thehill.com/policy/technology/458170-ice-renews-contract-with-palantir.
33. Haining, R. and Law, J. (2007) 'Combining police perception with police records of serious crime records of serious crime areas: a modelling approach'. J.R. Statist. Soc. 170,4: 1019-1034.
34. Upturn (2016) 'Stuck in a Pattern, Early evidence on "predictive policing" and civil rights'. Washington DC: Upturn.
35. Improvements have mostly been to resolution, storage capacity, cheaper hardware and improved wireless networking means they can be installed and monitored affordably.
36. Home Office (2018) 'Biometrics Strategy'. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf.
37. Buolamwini, J. and Gebru, T. (2018) 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification'. Proceedings of Machine Learning Research 81:1–15; see also 'Gender Shades', available at: http://gendershades.org/overview.html.
38. Dearden, L. (2019) 'Police stop people for covering their faces from facial recognition camera then fine man £90 after he protested'. The Independent. Available at: https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html.
39. Deutsche Welle (2017) 'G20: Hamburg police seek help to find 'Black Bloc' riot activists'. Available at: https://www.dw.com/en/g20-hamburg-police-seek-help-to-find-black-bloc-riot-activists/a-41838696.
40. The Hamburg Commissioner for Data Protection and Freedom of Information (2019) 'The protection of privacy as a challenge for the 21st century – digital development needs data protection'. Available at: https://datenschutz-hamburg.de/assets/pdf/2019-02-21-press-release.pdf.
41. Davies, B et al. (2018) 'An evaluation of south wales police's use of automated facial recognition'. Cardiff University. Available at: http://afr.south-wales.police.uk/cms-assets/resources/uploads/AFR-EVALUATION-REPORT-FINAL-SEPTEMBER-2018.pdf.
42. London Ethics Panel, Mayor of London (2019) 'Ethics Panel sets out future framework for facial recognition software'. Available at: https://www.london.gov.uk/press-releases/mayoral/future-framework-for-facial-recognition-software.
43. Liberty (2019) 'I resist racial recognition'. Available at: https://www.libertyhumanrights.org.uk/resist-facial-recognition.
44. Rosenberg, T. (2019) 'Oakland Passes Facial Recognition Ban'. Oakland Privacy. Available at: https://oaklandprivacy.org/2019/05/14/san-francisco-approves-oversight-of-surveillance-tech-and-becomes-1st-municipality-in-the-country-to-ban-the-use-of-facial-recognition/.
45. See http://news.bbc.co.uk/1/hi/uk_politics/6902543.stm.
46. Jansen, F. (2018) 'Data Driven Policing in the Context of Europe'. Available at: https://datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-Data-Driven-Policing-EU.pdf.
47. Jansen, F. (2018) 'Data Driven Policing in the Context of Europe'. Available at: https://datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-Data-Driven-Policing-EU.pdf.
48. Stopwatch and Liberty (2017) ''Driving While Black': Liberty and StopWatch's briefing on the discriminatory effect of stop and search powers on our roads'. London: Liberty.
49. Meister, A. (2019) 'Brandenburg: Top officials demand stop the registration plate'. Netzpolitik. Available at: https://netzpolitik.org/2019/brandenburg-spitzenbeamter-fordert-stopp-der-kennzeichenerfassung-und-wird-versetzt/.
50. An independent expert commission on antigypsyism has been established in Germany to assess the extent of the discrimination.

51. Interestingly while originally introduced to scan for a watch-list of number-plates, this ANPR system ended up being used to bulk capture every number-plate and store it for an unknown period of time.
52. 'Speaker Identification Integrated Project Factsheet' (2019). Available at: https://cordis.europa.eu/project/rcn/188607/factsheet/en.
53. Kofman, A. (2018) 'Finding your voice', The Intercept. Available at: https://theintercept.com/2018/01/19/voice-recognition-technology-nsa/
54. Page on Interpol Website, Speaker Identification Integrated Project. Available at: https://www.interpol.int/en/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/Speaker-Identification-Integrated-Project-SIIP.
55. Tatman, R. (2017) 'Gender and Dialect Bias in YouTube's Automatic Captions', First Workshop on Ethics in Natural Language Processing. Available at: http://www.ethicsinnlp.org/workshop/pdf/EthNLP06.pdf/.
56. There are currently no studies available looking at bias in speaker identification.
57. Identification Service, BKA website. Available at: https://www.bka.de/EN/OurTasks/SupportOfInvestigationAndPrevention/IdentificationService/identificationService_node.html.
58. Metropolitan Police (2018) 'Met develops mobile fingerprint device to save time and public money'. Available at: http://news.met.police.uk/news/met-develops-mobile-fingerprint-device-to-save-time-and-public-money-317200.
59. Home Office (2018) 'Police trial new Home Office mobile fingerprint technology'. Available at: https://www.gov.uk/government/news/police-trial-new-home-office-mobile-fingerprint-technology
60. See: S v Marper v the UK (Applications nos. 30562/04 and 30566/04). Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]}.
61. See: Privacy International Social Media Intelligence explainer. Available at: https://privacyinternational.org/explainer/55/social-media-intelligence.
62. Amnesty International (2018) 'Trapped in the Matrix: Secrecy, stigma, and bias in the Met's Gangs Database'. London: Amnesty International UK.
63. This occurs whenever someone makes a phone call, sends a text message, among other triggers.
64. IMSI stands for international mobile subscriber identifier, which is a unique number tied to your sim card.
65. Once your phone has connected to the police IMSI catcher, the tool is then able to access all communications to and from your phone including phone calls, SMS messages and potentially emails, although depending which apps are used and the strength of the encryption, there can be limits on what the police IMSI catcher is able to access. Some models even allow text messages to be edited or redirected during transmission.
66. Instead of intercepting communications to and from your phone, the police IMSI catcher can simply block your access to the mobile phone network. To individuals, it would appear that you had a good signal on your phone, but the signal strength is not that of the real mobile phone network, but of the police IMSI catcher. Some devices block all access, and for others, the blocking ends if any device tries to make an emergency call.
67. A number of IMSI catchers can be used in parallel, allowing police to triangulate a specific mobile phones location.
68. IMEI stands for international mobile equipment identifier, which is a unique number tied to a physical handset or mobile device.
69. GSM Association (2018) 'Access to Mobile Services and Proof of Identity 2019: Assessing the impact on digital and financial inclusion'. Available at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/ProofofIdentity2019_WebSpreads.pdf.
70. Wikileaks (2016) 'Aappro Security and defence: Company Brochure'. Available at: https://wikileaks.org/spyfiles/docs/AAPPRO_2011_AappSecuand_en.html.
71. Ofcom (2019) 'Radio frequency jammers'. Available at: https://www.ofcom.org.uk/spectrum/interference-enforcement/spectrum-offences/jammers.
72. Access Now (2016) 'Primer on internet shutdowns and the law'. Available at: https://www.ohchr.org/Documents/Issues/Expression/Telecommunications/AccessPart_I.docx.

73. Soghoian, C. (2013) 'Before the LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens'. Available at: https://www.aclu.org/sites/default/files/assets/libe-testimony-csoghoian.pdf.

74. StopWatch (2019) 'Call It Off: Are police searching mobile phones illegally'. Available at: http://www.stop-watch.org/uploads/documents/Call_it_Off_-_Are_police_searching_mobile_phones_illegally.pdf.

75. Privacy International (2019) 'What types of data can law enforcement extract from my phone?'. Available at: https://privacyinternational.org/blog/2840/what-types-data-can-law-enforcement-extract-my-phone.

76. Privacy international (2019) 'What types of data can law enforcement extract from my phone?' Available at: https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf.

77. Gallagher, R. (2018) 'Airport police demanded an activist's passwords. He refused. Now he faces prison in the UK'. The Intercept. Available at: https://theintercept.com/2017/09/23/police-schedule-7-uk-rabbani-gchq-passwords/.

78. Via calendar apps.

79. Lum, C., Koper, C., Merola, L., Scherer, A. and Reioux, A. (2015) Existing and Ongoing Body Worn Camera Research: Knowledge Gaps and Opportunities. Virginia: George Mason University Centre for Evidence-Based Crime Policy.

80. Henstock, D. et al. (2017) 'Testing the effects of police body-worn cameras on use of force during arrests: A randomised controlled trial in a large British police force'. European Journal of Criminology, 14(6).

81. Flight, S. Amsterdam Police (2019) 'Evaluatie pilot bodycams Politie Eenheid Amsterdam 2017-2018'. Amsterdam Police. Available at: https://www.politie.nl/binaries/content/assets/politie/nieuws/2019/pw93a.pdf

82. Ariel, B. et al. (2015) 'The Effect of Police Body-Worn Cameras on Use of Force and Citizens' Complaints Against the Police: A Randomized Controlled Trial'. Journal of Quantitative Criminology 31(3): 509–535.

83. Yokum, A. et al. (2017) 'Evaluating the Effects of Police Body-Worn Cameras: A Randomized Controlled Trial'. The Lab DC. Available at: https://bwc.thelab.dc.gov/TheLabDC_MPD_BWC_Working_Paper_10.20.17.pdf.

84. Henstock, D. et al. (2017) 'Testing the effects of police body-worn cameras on use of force during arrests: A randomised controlled trial in a large British police force'. European Journal of Criminology, 14(6).

85. 'Rashan Charles, a 20 year old black man, died following restraint by Metropolitan Police officers in Hackney, East London in the early hours of Saturday 22 July 2017. Concerning CCTV footage of the restraint was widely circulated, and his death has since received significant public attention and concern.' Further information on this case is available on the INQUEST website: https://www.inquest.org.uk/rashan-charles-opening.

86. Babuta, A. et al. (2019) 'Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges'. RUSI. Available at: https://rusi.org/publication/whitehall-reports/machine-learning-algorithms-and-police-decision-making-legal-ethical.

87. Bundesministerium des Innern (2018) 'Polizei 2020 White Paper'. Available at: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2018/polizei-2020-white-paper.pdf?__blob=publicationFile&v=1.

88. Dodd, V. (2018) 'Police super-database prompts Liberty warning on privacy'. The Guardian. Available at: https://www.theguardian.com/uk-news/2018/oct/01/police-super-database-prompts-liberty-warning-on-privacy.

89. Jansen, F. (2018) 'Data Driven Policing in the Context of Europe'. Data Justice Lab.

90. Jansen, F. (2018) 'Data Driven Policing in the Context of Europe'. Data Justice Lab.

91. German Constitutional Court (2006) 'Press release No. 40/2006'. Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2006/bvg06-040.html.

92. Jefferson, B.J. (2018) 'Predictable Policing: Predictive Crime Mapping and Geographies of Policing and Race'. Annals of the American Association of Geographers, 108 (1): 1-16.

93. Evidence given by Chief Constable Michael Barton of Durham Constabulary to Law Society Commission on the Uses of Algorithms in the Criminal Justice System. See: Veale, M. at al. Law Society of England and Wales (2019) 'Algorithms in the Criminal Justice System'. Available at: https://www.lawsociety.org.uk/support-services/research-trends/algorithm-use-in-the-criminal-justice-system-report/.

94. Jefferson, B.J. (2018) 'Predictable Policing: Predictive Crime Mapping and Geographies of Policing and Race'. Annals of the American Association of Geographers, 108(1): 1-16.

95. Ibid, 5.

96. Machine learning is a branch of Artifical Intelligence focused on building computer systems that learn directly from examples, data and experience rather than following pre-programmed rules. For more information and examples see: https://royalsociety.org/-/media/policy/projects/machine-learning/publications/machine-learning-introduction.pdf

97. Amnesty International (2018) 'Trapped in the Matrix: Secrecy, stigma, and bias in the Met's Gangs Database'. London: Amnesty International UK.

98. See "In the United Kingdom however, deployments of very similar technology have a much longer history. ProMap, built by researchers at the Jill Dando Institute of Crime Science, University College London around 2004, 120 was deployed and evaluated by the Home Office in the East Midlands in 2005/6." Veale, M. at al. (2019) 'Algorithms in the Criminal Justice System'. Law Society of England and Wales. Available at: https://www.lawsociety.org.uk/support-services/research-trends/algorithm-use-in-the-criminal-justice-system-report/.

99. Uptunr (2016) 'Stuck in a Pattern, Early evidence on "predictive policing" and civil rights'. Washington DC: Upturn. Available at: https://www.upturn.org/reports/2016/stuck-in-a-pattern/.

100. Experian factsheet. Available at: https://web.archive.org/web/20170924093105/ http://www.experian.com/corporate/experian-corporate-factsheet.html.

101. See: Privacy International (2018) 'Submission to the Information Commissioner–request for an assessment notice of data brokers Experian & Equifax'. Available at: https://privacyinternational.org/sites/default/files/2018-11/08.11.18%20Final%20 Complaint%20Experian%20%26%20Equifax.pdf.

102. Willems, D. (2014) 'CAS: Crime Anticipation System'. Presentation. Available at: https://event.cwi.nl/mtw2014/media/files/ Willems,%20Dick%20-%20CAS%20Crime%20anticipation%20system%20_%20predicting%20policing%20in%20Amsterdam.pdf.

103. Oosterloo, S. at al. (2017) 'The Politics and Biases of the "Crime Anticipation System" of the Dutch Police'. Available at: http://ceur-ws.org/Vol-2103/paper_6.pdf.

104. See the description of Richard Lewis, deputy chief constable of South Wales police: "The tech is given to us as a sealed box [..] We have no input — whatever it does, it does what it does." Nilsson, P. (2018) 'How UK police are using facial recognition software'. Financial Times. Available at: https://www.ft.com/content/06c46942-cc7d-11e8-b276-b9069bde0956.

105. Catt v UK, European Court of Human Rights (Application no. 43514/15). Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-189424%22]}.

106. Babuta, A. et al. (2019) 'Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges'. RUSI. Available at: https://rusi.org/publication/whitehall-reports/machine-learning-algorithms-and-police-decision-making-legal-ethical.

107. "Common themes identified in those comments included complaints about [...] training being sometimes non-existent". Kearns, I. et al. (2019) 'Data-driven policing and public value'. Police Federation. Available at: http://www.police-foundation.org.uk/2017/wp-content/uploads/2010/10/data_driven_policing_final.pdf.

108. Babuta, A. et al. (2019) 'Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges'. RUSI. Available at: https://rusi.org/publication/whitehall-reports/machine-learning-algorithms-and-police-decision-making-legal-ethical.

109. EDRI members list: https://edri.org/members/.

110. Surveillance Studies Academic Network Map: https://www.surveillance-studies.net/?p=1122.

Data-driven policing: the hardwiring of discriminatory policing practices across Europe

Across Europe we are witnessing the increased use of technologies to assist policing and wider law enforcement practices. While some of these technologies are not new, law enforcement's increased resort to data sharing and analytics, and predictive policing tools to direct policing resources has concerning implications for minority ethnic and marginalised communities.

This report explains the potential effects of the increased use of data-driven technologies for minority groups and communities. The introduction of new technology is negatively impacting ethnic minority communities in three ways: 1) the impact of new technologies to identify, surveil and analyse will be disproportionately felt by minority ethnic communities, as they are already over-policed; 2) many algorithmically driven identification-technologies disproportionately mis-identify people from black and other minority ethnic groups; and 3) predictive policing systems are likely to present geographic areas and communities with a high proportion of minority ethnic people as 'risky' and subsequently, foci for police attention.

The European Network Against Racism (ENAR) is the only pan-European network combining racial equality advocacy with building a strong network of anti-racist organisations across Europe. We ensure that laws and policies address racism and reflect the experiences of racialised people. We provide a unique space for organisations to connect and exchange strategies on how to combat racism and support our communities.

european network against racism aisbl

european network against racism aisbl
Tel: +32 (0)2 2 29 3 570 • E -mail : info@enar-eu.org
Facebook: /ENAREurope • Twitter: @ENAREurope • Web: www.enar-eu.org